



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/038,169	01/02/2002	Dan Boneh	200634-0096-00-US (425599)	7811
23973 7590 11/24/2009 DRINKER BIDDLE & REATH ATTN: INTELLECTUAL PROPERTY GROUP ONE LOGAN SQUARE 18TH AND CHERRY STREETS PHILADELPHIA, PA 19103-6996			EXAMINER TO, BAOTRAN N	
			ART UNIT 2435	PAPER NUMBER
			MAIL DATE 11/24/2009	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/038,169	<b>Applicant(s)</b> BONEH ET AL.	
	<b>Examiner</b> BaoTRAN N. To	<b>Art Unit</b> 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 07/06/2009.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 32-55 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 32-55 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. This Office action is in response to the Applicant's Amendment filed 07/06/2009.  
Claims 1-31 are previously canceled.  
Claims 32, 42-44, and 50-55 are amended.  
Claims 32-55 are presented for examination.

### ***Response to Arguments***

2. Applicant's arguments with respect to claims 32-42, 44-50, and 53-55 have been considered but are moot in view of the new ground(s) of rejection.

In response to applicant's arguments, the recitation "does not secure by encrypting, hashing, or keyed hashing the data received from the web before it is stored" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Applicant's arguments filed 07/06/2009 with respect to Claims 43, 51, and 52 have been fully considered but they are not persuasive.

Applicant appears to argue that "Rollins does not disclose or suggest an appliance for receiving a cookie provided by a separate web server environment, securing the cookies against tampering at the client, without providing means to the client to unsecure the cookies" (Page 14 of Remarks).

This argument is not persuasive because Rollins clearly discloses customer information stored on wallet server 714, client 703 or IOM 708 may be encrypted. For example, in the situation where **client information is stored in a wallet cookie on client 703 or IOM 708, an encrypted wallet cookie may be used to protect the client information**. Encrypted cookies may be use in combination with, or as an alternative to using secure communications links 710, 716 and 720. For example, if SSL is used to encrypt data transmitted over communications links 710, 716 and 720, messages are encrypted before being sent and then decrypted upon receipt. Because **the wallet cookie is encrypted separately before it is prepared for transmission, it will still be encrypted after receipt by the user's computer**. In this situation, customer information is encrypted twice (col. 20, lines 12-25). As explained above, the wallet cookie is still encrypted after receipt by the user's computer. Therefore, the encrypted wallet cookie is against tampering at the client. Rollins further discloses the encrypted cookie will be resent by the user's web browser to the proxy server each time the user accesses a web page on that merchant's website via the proxy server (col. 20, lines 40-43).

For at least the above reasons, the 102 rejection for Claims 43 and 51 is maintained.

Applicant further argues that “Wessman in view of Johnson, whether individually or in any possible combination, do not disclose, suggest, or render obvious at least a web server environment that stores data received from the web and does not secure the received data before it is stored, or a transparent encryption appliance comprising a processor that identifies a password contained in a data transaction, secures the password, replaces in the data transaction the identified password with the secured password, and provides the data transaction with secured password to the web server environment” (Page 16 of Remarks).

Examiner respectfully disagrees. Wessman discloses a transparent encryption appliance for protecting sensitive data contained in the data stored in the server environment (Figures 1 and 2, element 112), comprising: at least one network interface for coupling to at least one network and communicating with the one or more clients via the at least one network (Figures 1 and 2, interface between element 110 and 112); a server interface for coupling to the server environment, wherein the server interface and the at least one network interface communicate using the same communications protocol (Figures 1 and 2, interface between element 112 and 118); and a processor coupled to the at least one network interface and the server interface for at least one of securing and unsecuring data (Figures 1 and 2, element 112), wherein: securing data comprises: identifying first sensitive data contained in a data transaction received through the at least one network interface (col. 1, lines 15-17); securing the sensitive data by at least one of encrypting, hashing, and keyed hashing (Figure 6, element 602); replacing in the data transaction the identified sensitive data with the secured sensitive

data (Figure 6, element 610, col. 1, lines 15-17 and col. 6, line 9); and providing the data transaction including the secured sensitive data to the server environment, wherein the secured sensitive data is stored in the server environment (Figure 6, elements 606 and 612, col. 6, lines 10-12); and wherein, responsive to a request (a request from client 110) received through the at least one network interface of the appliance for an action requiring authorization, (Figure 7, element 702, col. 6, lines 17-18), retrieves a secured data previously secured by the appliance and stored by the data server (Figure 7, element 704, col. 6, lines 18-19). Wessman does not disclose sensitive data as password and wherein, responsive to a request received through the at least one network interface of the appliance for an action requiring authorization, the web server environment obtains the secured password from the provided data transaction, compares the obtained secured password to a previously stored secured password, and authenticates the action requiring authorization in the case the obtained secured password matches the previously stored secured password. However, sensitive data as password (Abstract) and wherein, responsive to a request received through the at least one network interface of the appliance for an action requiring authorization, the web server environment obtains the secured password from the provided data transaction, compares the obtained secured password to a previously stored secured password (Figure 1B, step S15B, col. 7, lines 30-35), and authenticates the action requiring authorization in the case the obtained secured password matches the retrieved previously stored secured password (Figure 1B, steps S17B and S18B, col. 7, lines 40-44). Therefore, it would have been obvious at the time the invention was made to one of

ordinary skill in the art at the time the invention was made to have incorporated Johnson's reference within Wessman to include above features in order to verify the web customer's identity (Johnson, col. 7, lines 43-44). Thus, the combination of Wessman and Johnson discloses "at least a web server environment that stores data received from the web and does not secure the received data before it is stored, or a transparent encryption appliance comprising a processor that identifies a password contained in a data transaction, secures the password, replaces in the data transaction the identified password with the secured password, and provides the data transaction with secured password to the web server environment" recited in claim 52.

For at least the above reasons, the 103 rejection for claim 52 is maintained.

### ***Claim Objections***

3. Claim 32 is objected to because of the following informalities: "the web" in line 2 should be --a web--. Appropriate correction is required.

Claim 52 is objected to because of the following informalities: "a web server environment" in lines 4 should be --the web server environment --. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

Art Unit: 2435

art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 32-41 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. After reviewing the original specification, the amended limitation "a web server environment that does not include the appliance" is not supported from the original specification.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 32-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 32 recites the limitation "retrieved from a database" in line 22. There is insufficient antecedent basis for this limitation in the claim. It is unclear that the database is the same database or not which is recited in line 17.

Claims 31-41 are also rejected because of dependency.



***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 43 and 51 are rejected under 35 U.S.C. 102(e) as being anticipated by Rollins (U.S. Patent 7,415,429 B2) hereinafter Rollins.

Regarding Claims 43 and 51, Rollins discloses a transparent encryption appliance/system for protecting a web server environment that does not secure cookies generated by the web server environment against cookies that have been tampered with at a client, comprising:

at least one network interface for coupling to at least one network and communicating with one or more clients via the at least one network (Figure 3, interface between elements 303 and 308);

a server interface for coupling to a web server environment, wherein the server interface and the at least one network interface communicate using the same communications protocol (SSL) (Figure 3, interface between elements 308 and 306 and Figures 7A and 7B, interface between elements 708, 706 and 714); and

a processor coupled to the at least one network interface and the server interface for securing and unsecuring cookies provided by the web server environment against tampering at the client (Figure 7, element 708 col. 20, lines 1-25), wherein:

securing a cookie comprises: identifying a cookie received through the server interface (col. 14, lines 66-67 and col. 18, lines 13-15); securing the cookie against tampering at the client by at least one of encrypting, hashing, and keyed hashing the cookie (col. 20, lines 1-25); and providing the secured cookie to a client computer through the at least one network interface without providing means to the client to unsecure the cookie, wherein the secured cookie is stored in the client computer (col. 20, lines 1-25); and

unsecuring a cookie comprises: responsive to a request received through the server interface for a cookie stored on a client computer (col. 18, lines 13-20), receiving from the client computer the secured cookie previously secured by the appliance corresponding to the requested cookie through the at least one network interface (col. 20, lines 38-46); unsecuring the received secured cookie by at least one of decrypting and hash verifying (col. 20, lines 16-21); and providing the unsecured cookie through the server interface (col. 18, lines 61-65).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2435

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 32-33, 35-41, 44, 46-49, and 52-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wessman (U.S. Patent 7,111,005 B1) hereinafter Wessman in view of Johnson (U.S. Patent 6,898,577 B1) hereinafter Johnson.

Regarding Claims 32, 44, 53, and 55, Wessman discloses a transparent encryption appliance/system/method/medium that does not store data for protecting data received from the client stored by a server environment that does not secure by encrypting, hashing, or keyed hashing the data received from the client before it is stored (Figures 1 and 2), comprising:

at least one network interface for coupling to at least one network and communicating with one or more clients via the at least one network (Figures 1 and 2, interface between elements 110 and 112);

a server interface for coupling to a server environment (Figures 1 and 2, interface between element 112 and 118), wherein the server interface and the at least one network interface communicate using the same communications protocol (Figures 1 and 2, interface between element 112 and 118); and

a processor coupled to the at least one network interface and the server interface for at least one of securing and unsecuring data (Figures 1 and 2, element 112), wherein:

securing data comprises: identifying first sensitive data contained in a data transaction received through the at least one network interface (col. 1, lines 15-17);

securing the sensitive data by at least one of encrypting, hashing, and keyed hashing (Figure 6, element 602); replacing in the data transaction the identified sensitive data with the secured sensitive data (Figure 6, element 610, col. 1, lines 15-17 and col. 6, line 9); and providing the data transaction including the secured sensitive data to the server environment, wherein the secured sensitive data is stored in a database by the server environment (Figure 6, elements 606 and 612, col. 6, lines 10-12); and

unsecuring data comprises: responsive to a request (a request from client 110) received through the at least one network interface for sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data (Figure 7, element 702, col. 6, lines 17-18), receiving from the server environment the secured sensitive data corresponding to the requested data (Figure 7, element 704, col. 6, lines 18-19); unsecuring the received secured data by at least one of decrypting and hash verifying (Figure 7, element 712, col. 6, lines 31-32); and providing the unsecured sensitive data through the at least one network interface (Figure 7, element 714, col. 6, lines 32-33).

Wessman does not explicitly disclose a server interface for coupling to a web server environment that does not include the appliance.

However, Johnson expressly discloses a server interface for coupling to a web server environment that does not include the appliance (Figure 4, col. 13, line 37 - col. 14, line 4).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art at the time the invention was made to have incorporated

Johnson's reference within Wessman to include above feature in order to verify the web customer's identity (Johnson, col. 7, lines 43-44).

Regarding Claim 33, the combination of Wessman and Johnson discloses the limitations of Claim 32 above. Wessman further discloses wherein: in securing data the data transaction is received through a first interface (Figures 6); and

in unsecuring data the request is received, and the unsecured data is provided through, the first interface or a second interface (Figure 7).

Regarding Claims 35 and 46, the combination of Wessman and Johnson discloses the limitations of Claim 32 above. Wessman further discloses wherein the received data transaction is one of a cleartext transaction and a Hypertext Transfer Protocol (HTTP) transaction (Figure 6, element 602).

Regarding Claim 36, the combination of Wessman and Johnson discloses the limitations of Claim 32 above. Wessman further discloses wherein the at least one network is at least one of the Internet, a wired network type, a wireless network type, a hybrid network type, an independent network, a proprietary network, or a back plane network (Figures 1 and 2).

Regarding Claims 37 and 47, the combination of Wessman and Johnson discloses the limitations of Claim 32 above. Wessman further discloses a key storage

for storing at least one cryptographic key for use in at least one of the securing and unsecuring of data (Figure 1, elements 116 and 120, col. 3, lines 52-58).

Regarding Claims 38-39 and 48, the combination of Wessman and Johnson discloses the limitations of Claim 32 above. Wessman further discloses above a user interface for use in loading the at least one key into the key storage and wherein the user interface is further for use in specifying access controls to the stored keys (Figure 1, elements 116 and 120, col. 3, lines 52-58).

Regarding Claims 40-41 and 49, the combination of Wessman and Johnson discloses the limitations of Claim 32 above. Wessman further discloses above a user interface for use in specifying one or more fields containing the sensitive data wherein the one or more fields are identified by one or more regular expressions (col. 5, lines 30-63).

Regarding Claim 54, the combination of Wessman and Johnson discloses the limitations of Claim 53 above. Wessman further discloses after the storing step: responsive to request for at least a portion of the sensitive data, retrieving the stored secured sensitive data corresponding to the request sensitive data (Figure 7, element 704, col. 6, lines 18-19); unsecuring the retrieved sensitive data by at least one of decrypting and hash verifying (Figure 7, element 712, col. 6, lines 31-32); and providing

the unsecured sensitive data to fulfill the request (Figure 7, element 714, col. 6, lines 32-33).

Regarding Claim 52, Wessman discloses a system for protecting sensitive data stored in a server environment, (Figures 1 and 2), comprising:

- one or more clients coupled to at least network (Figures 1 and 2, element 110);

- a server environment that stores data received from the client and does not secure by encrypting, hashing, or keyed hashing the data received from the client before it is stored (Figures 1 and 2, element 118), and a transparent encryption appliance for protecting sensitive data contained in the data stored in the server environment (Figures 1 and 2, element 112), comprising:

- at least one network interface for coupling to at least one network and communicating with the one or more clients via the at least one network (Figures 1 and 2, interface between element 110 and 112);

- a server interface for coupling to the server environment, wherein the server interface and the at least one network interface communicate using the same communications protocol (Figures 1 and 2, interface between element 112 and 118);
- and

- a processor coupled to the at least one network interface and the server interface for at least one of securing and unsecuring data (Figures 1 and 2, element 112),
- wherein:

securing data comprises: identifying first sensitive data contained in a data transaction received through the at least one network interface (col. 1, lines 15-17); securing the sensitive data by at least one of encrypting, hashing, and keyed hashing (Figure 6, element 602); replacing in the data transaction the identified sensitive data with the secured sensitive data (Figure 6, element 610, col. 1, lines 15-17 and col. 6, line 9); and providing the data transaction including the secured sensitive data to the server environment, wherein the secured sensitive data is stored in the server environment (Figure 6, elements 606 and 612, col. 6, lines 10-12); and

wherein, responsive to a request (a request from client 110) received through the at least one network interface of the appliance for an action requiring authorization, (Figure 7, element 702, col. 6, lines 17-18), retrieves a secured data previously secured by the appliance and stored by the data server (Figure 7, element 704, col. 6, lines 18-19).

Wessman does not disclose sensitive data as password and wherein, responsive to a request received through the at least one network interface of the appliance for an action requiring authorization, the web server environment obtains the secured password from the provided data transaction, compares the obtained secured password to a previously stored secured password, and authenticates the action requiring authorization in the case the obtained secured password matches the previously stored secured password.

However, sensitive data as password (Abstract) and wherein, responsive to a request received through the at least one network interface of the appliance for an



action requiring authorization, the web server environment obtains the secured password from the provided data transaction, compares the obtained secured password to a previously stored secured password (Figure 1B, step S15B, col. 7, lines 30-35), and authenticates the action requiring authorization in the case the obtained secured password matches the retrieved previously stored secured password (Figure 1B, steps S17B and S18B, col. 7, lines 40-44).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Johnson's reference within Wessman to include above features in order to verify the web customer's identity (Johnson, col. 7, lines 43-44).

8. Claims 34, 42, 45, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wessman and Johnson as Claims 32 and 44 and further in view of Rollins (U.S. Patent 7,415,429 B2) hereinafter Rollins.

Regarding Claims 34 and 45, Wessman discloses the limitations of Claim 32 above. Wessman does not disclose wherein the processor manages SSL traffic and handles computations that support SSL connections, wherein at least one of: in securing data the data transaction is received via a first SSL connection and SSL computations are completed before identifying the first sensitive data contained in the data transaction; and in unsecuring data the unsecured data is provided via a second SSL connection.

However, Rollins expressly disclose the above features (Figure 7, elements 710, 716, and 720, col. 20, lines 12-25).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art at the time the invention was made to have incorporated Rollins's reference within Wessman and Johnson to include SSL connection in order to provide enhanced security.

Regarding Claims 42 and 50, Wessman discloses the limitations of Claim 32 above. Wessman does not disclose wherein the appliance secures and unsecures web cookies provided by the web server environment, wherein: securing a cookie comprises: identifying a cookie received through the server interface; securing the cookie by at least one of encrypting, hashing, and keyed hashing the cookie; and providing the secured cookie to one of the one or more clients through the at least one network interface, wherein the secured cookie is stored in the client; and unsecuring the cookie comprises: responsive to a request received through the server interface for the cookie stored on a client, receiving from the client the secured cookie corresponding to the requested cookie through the at least one network interface; unsecuring the received secured cookie by at least one of decrypting and hash verifying; and providing the unsecured cookie through the server interface.

However, Rollins expressly discloses securing a cookie comprises: identifying a cookie received through the server interface (col. 14, lines 66-67 and col. 18, lines 13-15); securing the cookie by at least one of encrypting, hashing, and keyed hashing the

cookie (col. 20, lines 1-25); and providing the secured cookie to a client computer through the at least one network interface, wherein the secured cookie is stored in the client computer (col. 20, lines 1-25); and

unsecuring a cookie comprises: responsive to a request received through the server interface for a cookie stored on a client computer (col. 18, lines 13-20), receiving from the client computer the secured cookie corresponding to the requested cookie through the at least one network interface (col. 20, lines 38-46); unsecuring the received secured cookie by at least one of decrypting and hash verifying (col. 20, lines 16-21); and providing the unsecured cookie through the server interface (col. 18, lines 61-65).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art at the time the invention was made to have incorporated Rollins's reference within Wessman and Johnson to include cookie in order to allow a web server to identify repeat users or customers and to allow the web server to customize its content based upon the user's preferences that are stored in the cookie (Rollins, col. 13, lines 14-18).

### ***Conclusion***

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

***Contact Information***

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is (571)272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2435

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/B. N. T./

Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435